EXPLANATORY STATEMENT

Issued by authority of the Minister for Home Affairs and the Minister for Cyber Security

Cyber Security Act 2024

Cyber Security (Ransomware Payment Reporting) Rules 2025

Legislative Authority

The *Cyber Security (Ransomware Payment Reporting) Rules 2025* (the Rules) are made under sections 26 and section 27 of the *Cyber Security Act 2024* (the Act).

Purpose and background

Part 3 of the Act imposes a mandatory reporting obligation for certain entities who are impacted by a cyber incident, and who have provided or are aware that another entity has provided on their behalf a payment or benefit to an entity seeking to benefit from the impact of the cyber security incident (a ransomware payment).

The mandatory reporting obligation applies to reporting business entities. These are either responsible entities for a critical infrastructure asset under the *Security of Critical Infrastructure Act 2018* (SOCI Act), or another entity that meets the criteria of a reporting business entity in subsection 26(2) of the Act. That subsection provides that an entity will be subject to the reporting obligation if, at the time the ransomware payment is made, the entity:

- is carrying on a business in Australia with an annual turnover threshold for the previous financial year that exceeds the turnover threshold for that year prescribed in the Rules, and is not a Commonwealth or State body, or a responsible entity for a critical infrastructure asset; or

- is a responsible entity for a critical infrastructure asset to which Part 2B of the SOCI Act applies.

Subsection 26(3) of the Act provides that Rules may prescribe the turnover threshold, or manner for determining the turnover threshold, for the purpose of enlivening the mandatory reporting obligation. For this purpose, the Rules establish a turnover threshold of $3 million. The Rules additionally establish a formula for determining the annual turnover threshold for businesses who have only operated for part of the previous financial year.

Part 3 of the Act additionally provides that entities subject to the mandatory reporting obligation must provide a ransomware payment report to the designated Commonwealth body within 72 hours of the making of a ransomware payment or becoming aware the payment has been made. The ransomware payment report must contain information specified in subsection 27(2) of the Act, which includes contact and business details of the entity that made the report, details about the cyber security incident, the demand made and payment provided, and any communications with the extorting entity.

The Rules also prescribes additional requirements to be observed when providing the details that must be contained in a ransomware payment report. Specifically, the Rules prescribe that the following information must be contained as part of a ransomware payment report for the purposes of subsection 27(2) of the Act:

- the business details required under paragraph 27(2)(a) must include an Australian Business Number for the reporting business entity, or the entity that made the report on the reporting business entity's behalf (paragraph 27(2)(b));

- information about the cyber security incident under paragraph 27(2)(c) should include when the incident occurred, the impact of the incident, the variant of ransomware used, the vulnerabilities that were exploited and other information that could assist a Commonwealth body or State body respond to the cyber security incident;

- information about the ransomware payment itself (paragraph 27(2)(d)) should include the quantum and method of the ransomware payment, or equivalent details if the payment was non-monetary; and

- information about the communications with the extorting entity (paragraph 27(2)(e)) should include the nature and timing of communications and a description of those communications.

The Rules commence on the later of the day after the Rules are registered, or the same time as Part 3 of the Act commences.

Consultation

The Rules are made by the Minister administering the Act in accordance with the requirements of subsection 87(3) and 87(4) of the Act. These subsection specify, the Minister, before making or amending Rules under the Act, must cause a notice to be published that:

- sets out the draft rules or amendments; and

- invites persons to make submissions to the Minister about the draft rules within a period not shorter than 28 days.

The Minister must also consider any submissions received during the period specified in the notice.

In accordance with these requirements, the draft Rules were published on the Department's website on 16 December 2024 and closed for submissions on 14 February 2025, with 37 submissions received. The majority of submissions were broadly supportive of the proposed Rules, with several stakeholders requesting the Department to publish further guidance material to assist businesses in complying with the reporting obligation.

To support the submissions process, the Department consulted across a broad cross-section of the economy, including peak bodies, government agencies and industry. The Department hosted 8 'Deep Dive' sessions in January and February 2025 for all of the Rules, with over 995 total

attendees, with each session averaging 124 attendees. The ransomware payment reporting sessions saw over 270 attendees across the two sessions.

In these circumstances, the Minister was satisfied that appropriate consultation was undertaken, in accordance with section 17 of the *Legislation Act 2003* because:

- persons likely to be affected by the Rules had an adequate opportunity to comment on the draft Rules for a period of at least 28 days, with significant consultation across the economy; and

- throughout the consultation process, affected persons did not raise any significant concerns regarding the ransomware payment reporting rules.

An Impact Analysis statement has been prepared by the Office of Impact Analysis for mandatory ransomware payment reporting as part of the Explanatory Memorandum for the Cyber Security Bill 2024 (OIA24-07090). The Impact Analysis of Mandatory Ransomware Payment Reporting was tabled in the Parliament as an attachment to the Bill's explanatory memorandum, and is available on the Parliament's website.[1]

Other matters

The Rules are a legislative instrument for the purposes of the *Legislation Act 2003* and are subject to disallowance.

Details of the Rules are set out in **Attachment A**.

A Statement of Compatibility with Human Rights provides that the Rules are compatible with human rights because it promotes the protection of human rights, and to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate to pursue the legitimate objective of national security and public order. The Statement is included at **Attachment B**.

[1] https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r7250

ATTACHMENT A

Details of the *Cyber Security (Ransomware Payment Reporting) Rules 2025*

Part 1 Preliminary

Section 1 Name

This section provides that the name of the instrument is the *Cyber Security (Ransomware Payment Reporting) Rules 2025*.

Section 2 Commencement

Section 2 provides for the commencement provisions of the Rules.

Subsection 2(1) provides that each provision of the Rules specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table.

The effect of column 2 is that the whole of the Rules will commence on the later of the start of:

- the day after the Rules are registered; and
- at the same time as Part 3 of the *Cyber Security Act 2024* (the Act) commences.

A note immediately under the table explains that the table relates only to the provisions of the Rules as originally enacted. The table will not be amended to deal with any later amendments of the Rules.

Subsection 2(2) provides that any information in column 3 of the table is not part of the Rules. Information may be inserted in this column, or information in it may be edited, in any published version of the Rules.

Section 3 Authority

This section provides that the Rules are made under the Act.

Section 4 Definitions

This section sets out the definition of terms used in the Rules.

The note in section 4 provides that the expressions cyber security incident, ransomware payment and reporting business entity, which are used in the Rules, are defined in section 8 of the Act.

This section also provides that the reference to ***Act*** is the *Cyber Security Act 2024*.

Part 2 Ransomware payment reporting obligations

Section 5 Simplified outline of this part

Section 5 provides a simplified outline for the reader regarding the operation of the Rules.

The simplified outline provides that an entity has an obligation to provide a ransomware payment report if an entity is a reporting business entity and is impacted by a cyber security incident, is impacted by a cyber security incident and has provided or is aware that another entity has provided on their behalf, a ransomware payment to an entity that is seeking to benefit from the impact or the cyber security incident.

The simplified outline further provides guidance to the reader on what is considered a responsible business entity under the Act**.** An entity is a reporting business entity if it is a responsible entity for a critical infrastructure asset to which part 2B of the *Security of Critical Infrastructure Act 2018* applies, or if an entity is carrying on a business in Australia with an annual turnover that exceeds the turnover threshold.

The final part of the simplified outline provides that particular information must be included in a ransomware payment report, including information relating to the cyber security incident, the demand made by the extorting entity and the ransomware payment. The information contained in the report must be in accordance with the requirements provided by the Rules.

Simplified outlines are included to assist readers to understand the substantive provisions. The outline for this part is not intended to be comprehensive, and readers should rely on the substantive provisions in the Rules.

Section 6 Turnover Threshold

Subsection 6(1) of the Rules specify, for the purpose of paragraph 26(3)(b) of the Act, that the turnover threshold for a business for the previous financial year is $3 million.

This threshold is established for the purposes of determining if an entity is a reporting business entity for the purpose of enlivening the mandatory reporting obligation in Part 3 of the Act. Part 3 of the Act provides that an entity will be subject to the ransomware payment reporting obligation if the entity is carrying on a business in Australia that meets the annual turnover requirement for the previous financial year.

Subsection 6(2) of the Rules specify, for the purposes of paragraph 26(3)(a) of the Act, a formula for determining the turnover threshold if a business has only been carried out for a part of the previous financial year.

The formula prescribed by section 6(2) is $3 million multiplied by the quotient of the number of days in the part divided by number of days in the previous financial year. Number of days in the part refers to the number of days an entity carried on a business for in the previous financial year.

Where the annual turnover of a reporting business entity is greater than or equal to the result of the formula, a reporting business entity is captured by the mandatory reporting obligation. Conversely, where the annual turnover of a reporting business entity is less than the result of the formula, a reporting business entity is not captured by the mandatory reporting obligation.

The $3 million threshold was selected to align with existing thresholds familiar to industry and to balance the regulatory burden with the benefit of the reporting data. Similar thresholds include section 6D of the *Privacy Act 1988*, where a small business is defined as earning $3 million or less, during a previous financial year and are generally exempt from the reporting requirements for notifiable data breaches.

The $3 million threshold captures approximately 6.56% of registered Australian businesses and appropriately balances the impact on those Australian businesses, particularly small business, whilst meeting the policy intent of the Act, to build the Government's threat picture on the impacts of ransomware and cyber extortion. Small business, or entities with a lower annual turnover threshold, may not have the capability, capacity or resources to remediate the impact of cyber security incidents.

Modelling in the impact analysis shows that for an entity with an annual turnover of $3 million, the initial compliance costs for that captured entity is calculated at $276.80 per entity (less than 0.001% of that organisation's turnover). This shows that there will not be any significant impacts on individual entities, with the value of the mandatory reports providing considerable benefits across the whole-of-economy.

Section 7 Requirements for information that ransomware payment report must contain

Section 7 prescribes requirements for information that a ransomware payment report given by a reporting business entity in relation to a ransomware payment must contain.

Subsection 7(1) prescribes, for the purposes of subsection 27(2) of the Act, information requirements for a ransomware payment report given by a reporting business entity. Section 27(2) specifies the information that must contained in the ransomware payment report. The purpose of section 7 is to prescribe the specific information relating to the ransomware payment report for this purpose.

The note under subsection 7(1) reminds the reader that Part 3 of the Act only requires information to be given to the extent that the reporting business entity knows or is able, by reasonable search or enquiry, to find out within the 72 hour time period for giving the report.

Subsection 7(2) provides, for the purpose of paragraph 27(2)(a) of the Act, that a reporting business entity's contact and business details must include the entity's Australian Business Number (ABN) (if any) and address. Paragraph 27(2)(a) of the Act provides that if the reporting business entity made the payment, then the reporting business entity's contact and business details must be included in the ransomware payment report. The purpose of subsection 7(2) of the Rules is to prescribe the ABN as specific contact and business information relating to the reporting business entity that must be contained in the ransomware payment report.

Subsection 7(3) provides, for the purpose of paragraph 27(2)(b) of the Act, that contact and business details of an entity that made the payment on behalf of a reporting business entity must include the entity's ABN (if any) and address. Paragraph 27(2)(b) of the Act requires that if another entity made the payment on a reporting business entity, then that entity's contact and business details must be included in the ransomware payment report. The purpose of subsection 7(3) therefore is to prescribe the entity's ABN as specific contact and business information relating to the other entity that made the ransomware payment.

Subsection 7(4) prescribes, for the purpose of paragraph 27(2)(c) of the Act, what information about the cyber security incident, including its impact on the reporting business entity, a ransomware payment report must include. Subsection 7(4) prescribes the following information must be included for this purpose:

- when the incident occurred or is estimated to have occurred;
- when the reporting business entity became aware of the incident;
- the impact of the incident on the reporting business entity;
- the impact of the incident on the reporting business entity's customers;
- what variant (if any) of ransomware or other malware were used;
- what vulnerabilities (if any) in the reporting business entity's systems were exploited; and
- information that could assist the response to, mitigation or resolution of the cyber incident by a Commonwealth body or State body.

Section 27(2)(c) requires that a reporting business entity must provide information regarding the cyber security incident, including its impact on the reporting business entity. The purpose of subsection 7(4) of the Rules is to prescribe the specific information relating to the cyber security incident that must be contained in the ransomware payment report.

The information outlined in subsection 7(4) is useful for the Government to:

- understand which critical infrastructure assets, businesses, or sectors of the economy are being targeted by ransomware and cyber extortion;
- understand the impact on these entities;
- what variants of ransomware are being used where they have successfully been deployed and locked or blocked access to systems and data;
- what ransomware actors and cybercriminals appear to be most active, or have had the most success in deploying successful ransomware and cyber extortion demands to receive payments;

- common weaknesses that are exploited within a target's systems to facilitate a successful ransomware or cyber extortion payment; and

- where an entity goes to seek assistance from the Commonwealth or State, and how the Government can better assist within the incident response phase of a cyber security incident.

Collecting this information will support intelligence and law enforcement agencies in offensive cyber operations, but also assist the Government in disseminating tailored advice to industry and businesses, particularly small business, on how to uplift their cyber hygiene, protect and secure their data. This advice may also assist entities to remediate identified cyber security vulnerabilities that aggregated reports have identified are commonly exploited by extorting entities.

The note under subsection 7(4) reminds the reader that ransomware payment reports may only be used or disclosed for permitted purposes which include purposes relating to the response to, mitigation or resolution of the cyber security incident. The information must not be disclosed to a State body unless a Minister of the State or Territory has consented.

Subsection 7(5) provides, for the purpose of paragraph 27(2)(d) of the Act, that information about the demand made by the extorting entity must include the amount or quantum of the payment demanded, or if the ransomware payment is a non-monetary benefit, a description of the ransomware payment demanded. In addition, the ransomware payment report must also include details about the method of provision demanded. The purpose of subsection 7(5) is to prescribe the specific information relating to the demand made by the extorting entity that must be contained in the ransomware payment report.

Subsection 7(6) provides, for the purpose of paragraph 27(2)(e) of the Act, that information about the ransomware payment that must include the amount or quantum of the payment, or if the ransomware payment is a non-monetary benefit, a description of the ransomware payment. The ransomware payment report must also include method of provision. Section 27(2)(e) requires that a reporting business entity must provide specific information regarding the ransomware payment in the ransomware payment report. The purpose of subsection 7(6) is to prescribe the specific information relating to the ransomware payment that must be contained in the ransomware payment report.

The information required in subsection 7(6) may provide further details on the payment. For example, in the event a crypto currency payment was made, the details of the receiving wallet and other identifying details can be included. The Rules allow for flexibility in reporting, given the breadth of the types of ransomware and cyber extortion demands. Details on the payment quantum, type and methodology could benefit law enforcement operations and investigations, and will be fundamental to building a detailed understanding of the quantity and form of payment (or other benefit) being transferred to cyber threat actors. For example, this data could be used to analyse trends in payment methods for cyber extortion and to understand how various forms of payment method (such as cryptocurrency and newer technologies) are being used to transfer illicit funds.

Subsection 7(7) provides, for the purpose of paragraph 27(2)(f) of the Act, that the information about communications with the extorting entity relating to the incident, the demand and the ransomware payment given must include:

- the nature and timing of any communications between the entity and the extorting entity;
- a brief description of those communications (if any); and
- a brief description of any pre-payment negotiations undertaken in relation to the demand or ransomware payment.

Paragraph 27(2)(f) provides those communications with the extorting entity relating to the incident, the demand and the payment must be included in the ransomware payment report. The purpose of subsection 7(6) is to prescribe the specific information relating to communications with the extorting entity that must be contained in the ransomware payment report.

If a pre-payment negotiation has taken place, or the impacted entity has otherwise communicated with the extorting entity, this information could be useful for Government to learn how ransomware and cyber extortion criminals engage with their targets and may provide insight as to what actions they may take into the future.

ATTACHMENT B

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Cyber Security (Ransomware Payment Reporting) Rules 2025

This Disallowable Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Disallowable Legislative Instrument

Australia's cyber security landscape is evolving, with malicious activities targeting Australia becoming more frequent and sophisticated. The *Cyber Security Act 2024* (the Act) provides a clear legislative framework for whole-of-economy cyber security issues.

The Act imposes a mandatory reporting obligation for certain entities who are impacted by a cyber security incident, and who have provided or are aware that another entity has been provided on their behalf, a ransomware payment in connection with the cyber security incident (ransomware payment.

Subsection 26(3) of the Act provides that the *Cyber Security (Ransomware Payment Reporting) Rules 2025* (the Disallowable Legislative Instrument) may prescribe the annual turnover threshold, or the manner for determining the turnover threshold, to enliven the mandatory reporting obligation for relevant businesses.

Section 6 of the Disallowable Legislative Instrument establishes an annual turnover threshold of $3 million. Where a business earns $3 million or more during the previous financial year, they will be captured by the mandatory reporting obligation. Section 6 also sets out a formula to determine the turnover threshold for businesses that have operated for only part of a financial year. If the reporting business entity's turnover is greater than or equal to the result of the formula, then the reporting business entity is captured by the mandatory reporting obligation. Conversely, if the reporting business entity's turnover is less than the result of the formula, the reporting business entity is not captured by the mandatory reporting obligation.

Subsection 27(2) of the Act specifies what information a ransomware report must contain. Pursuant to subsection 27(2), section 7 of the Disallowable Legislative Instrument specifies particular information that a ransomware payment report must contain:

- The Australian Business Number for the reporting business entity, or the entity that made the report on the reporting business entity's behalf;
- Information about the cyber security incident: including, when the incident occurred or is estimated to have occurred, when the reporting business entity became aware of the incident, the impact of the incident on the reporting business entity's infrastructure and customers, what variants (if any) of ransomware or other malware were used, what vulnerabilities (if any) in the reporting business entity's systems were exploited and information that could assist with the response to, mitigation or resolution of the cyber security incident;

- The quantum and method of the payment demanded by the extorting entity and the quantum and method of the ransomware payment; and
- Additional information about the communications with the extorting entity, including the nature and timing of communications and a description of those communications or other pre-payment negotiations.

These requirements ensure the Government has access to valuable intelligence to enhance the national threat picture of the trends of ransomware payment reporting, allowing it to concentrate remediation, education and uplift efforts effectively.

It remains the compliance posture of the Department of Home Affairs to work in partnership with industry, to ensure regulated entities understand and can comply with their legal obligations through an 'education first' approach.

Human rights implications

This Disallowable Legislative Instrument does not engage any of the applicable rights or freedoms.

Conclusion

The Disallowable Legislative Instrument is compatible with human rights as it does not raise any human rights.

The Honourable Tony Burke MP
Minister for Home Affairs and Minister for Cyber Security